图书情报工作
第 62 卷 第 18 期 2018 年 9 月

社交网络中个人信息安全行为影响因素的实证研究*

王晰巍[1,2] 王雷[1] 贾若男[1] 王铎[1]
[1] 吉林大学管理学院 长春 130022 [2] 吉林大学大数据管理研究中心 长春 130022

摘要：[**目的/意义**]随着社交网络用户的逐渐增多，社交网络中个人信息安全行为研究对帮助社交网络用户更好地规避社交网络安全风险、推动社交网络平台开发商提高信息安全技术具有积极的作用。[**方法/过程**]基于社会认知和保护动机理论，构建社交网络个人信息安全行为影响因素模型，并运用问卷调查和结构方程方法对模型的适用性进行检验。[**结果/结论**]数据结果表明，反应效能是社交网络中个人信息安全保护行为最主要的影响因素，其次是感知威胁和自我效能对个人信息安全保护意愿产生正向影响，而回避行为对信息安全保护意愿产生消极影响，用户信息安全保护意愿对信息安全保护行为产生正向影响。

关键词：社交网络 个人信息安全 行为 影响因素
分类号：G250
DOI：10.13266/j.issn.0252-3116.2018.18.003

1 引言

近年来全球网络空间安全威胁呈现新的变化，一些新型网络威胁正呈现全球蔓延的态势。根据腾讯发布的《2017 年度互联网安全报告》显示，网络安全领域机遇与挑战并存，网络攻击、社交网络信息泄漏、诈骗等安全事件层出不穷，不断敲响民众数据和信息安全的警钟[1]。根据第 41 次中国互联网络发展状况统计报告显示，2017 年遭遇过网络安全事件的用户占比达到整体网民的 52.6%，这其中利用社交软件冒充好友进行诈骗占比为 48.4%[2]。国内外知名社交网络公司诸如 Linkedln、雅虎和网易等纷纷爆出用户信息被黑客盗取，导致成千上万的用户账户信息被不法分子所利用。社交网络用户不安全的信息行为是导致个人隐私泄露、被非法分子盗取的首要原因[3]。随着社交网络用户的增多，社交网络中个人信息安全行为成为产业界和学术界关注的新问题。

国内外相关学者近些年针对用户信息安全行为分别展开了相关研究。国外学者 A. Bandura 通过社会认知理论模型贴切地研究用户的信息安全行为[4]；A. C. Johnston 等学者从用户决定采取信息安全行为时进行研究，认为用户对社会环境的感知将影响其本身的行为意愿[5]；Y. Chen 等学者从中美两国语境下的个体在线安全行为方式对信息安全行为进行了比较[6]。国内学者张晓娟以隐私关注理论为基础，构建了隐私关注对智能手机用户信息安全行为意向的影响因素模型，对引入信任、隐私风险感知和以往经验 3 个关键影响因素进行深入研究[7]；王璐瑶基于恐惧诉求理论，构建了社交网络用户采纳隐私安全保护措施行为意愿的影响因素模型，对社交网络中用户个人信息安全的影响机制进行研究[8]；罗力提出有效保护社交网络个人信息安全的 3 种途径，包括加强立法保障和行业自律、提高社交网络企业的信息安全管理水平和提升用户信息安全素养[9]。从现有国内外学者的研究成果来看，现有成果大多集中于用户隐私安全保护和东西方信息安全行为意愿的对比研究，但是研究社交网络中用户信息安全行为的成果却相对很少，尤其是研究“回避行为”对用户的影响则更少。

本文在研究中试图解决以下 3 个方面的研究问题：①社交网络情境下用户信息安全行为的影响因素；②回避行为对用户信息安全行为的作用；③通过实证

* 本文系国家自然科学基金面上项目“信息生态视角下新媒体信息消费行为机理及服务模式创新研究”(项目编号：71673108)和“吉林大学高峰学科(群)建设项目”研究成果之一。

作者简介：王晰巍(ORCID：0000-0002-5850-0126)，副院长，大数据管理研究中心主任，教授，博士生导师，E-mail：wxw_mail@163.com；王雷(ORCID：0000-0002-0199-6343)，硕士研究生；贾若男(ORCID：0000-0002-4262-7982)，硕士研究生；王铎(ORCID：0000-0002-5060-7893)，博士研究生。

收稿日期：2018-02-11 修回日期：2018-04-27 本文起止页码：24-33 本文责任编辑：易飞

研究验证本文构建社交网络信息安全模型的实用性。本文以社会认知理论与保护动机理论为基础,构建社交网络中用户信息安全行为影响因素模型,从而在理论层面为社交网络中个人信息安全行为研究提供新的研究视角,实践层面上帮助社交网络用户更好地规避社交网络中存在的安全风险。

2 相关概念及理论基础

2.1 社交网络与用户个人信息安全

社交网络(social network sites,SNS)就是社会关系的网格化,本文所探讨的社交网络是以实名制为主要特征、以建立和管理个人或机构社会关系作为目的的网络平台[9]。国外对社交网络的定义大多是指一种社交工具,他们认为社交网络是一种以互联网为平台的服务,该服务使用户可以建立属于自己的网络空间,建立自己的好友圈,以及公开或半公开的供陌生人或朋友浏览、评论和转发的社交工具[10]。中国采用微博、微信和 QQ 空间作为社交网络工具的居多,国外以 Twitter 和 Facebook 等为典型代表。

社交网络用户个人信息安全,主要是指用户本身关于信息的安全问题。个人的年龄、性别、宗教信仰、思维方式、动机和文化背景等都会影响社交网络用户个人信息安全。随着互联网的快速发展,很多黑客从最开始的"入侵炫技"到后来的"黑客经济"[11],以及社交网络中存在的风险链接和网络诈骗的频频发生,导致人为因素对社交网络中个人的信息安全行为的影响越加凸显。

2.2 社会认知理论与社交网络安全行为

社会认知理论(social cognitive theory,SCT)认为社会心理是以一定的结构存贮于人的头脑中,结构及其部分之间具有相互关系;同时个人知识的获取通常受外界社会环境和个人经验影响;其核心观点是"三元交互"决定论,即环境、行为和人三者之间存在着动态的交互作用,并相互影响和互相依赖。社会认知理论概念提出者 B. E. Holt 认为所有人的行为都是以满足"感受、情感和欲望"的心理需要为基础[12]。其中,自我效能是社会认知理论中的一个重要概念,指在评估应对的过程中用户决定自己是否有能力去积极处理问题的自信程度[5,13]。A. Inkelesr 认为现代西方社会的人们具有高度的个人主义原则,他们在应对挑战方面有很强的自我效能感,往往会采取积极主动的态度去处理问题[14]。

当前中国用户面对社交网络用户安全问题时,往往采取"和谐"和"回避"的行为[15];且中国传统文化也一直"强调集体"应对和"依靠权威"来应对各种风险[16]。目前,国内很多学者忽略了从"回避性"这一角度来探讨社交网络用户信息安全行为,因此本文将"回避性"作为一个独立的变量引入模型,结合社会认知理论共同探讨用户的信息安全行为。

2.3 保护动机理论与社交网络安全行为

保护动机理论(protection motivation theory,PMT)框架分为 3 个部分,即信息源、认知中介过程和应对模式,具体指通过认知调节过程的威胁评估和应对评估来解释行为改变的过程,个体在此基础上作出相应决策。该理论认为信息源影响信息行为。R. W. Rogers 等曾经用它来研究安全行为,认为威胁评估和应对评估是保护动机理论中最重要的两个因素,威胁评估反映了个体对威胁易感性和威胁严重性的评估,应对评估则反映了个人对自我效能和反应效能的评估[17]。

当用户面对社交网络所带来的个人信息安全风险时,用户首先会判断自己经历这种威胁的可能性与这种威胁施加到自己身上所造成危害的严重性,然后再采取个人认为能够有效避免这种威胁的行为。除此之外,H. Liang 和 Y. Xue 等学者认为感知易感性和感知严重性能够通过中介变量感知威胁进而影响安全行为意愿,于是他们将感知威胁引入到保护动机理论的模型中[13]。许多学者已经通过若干实验来证明保护动机理论在研究社交网络用户行为方面起着重要的作用。鉴于这种情况,本文通过对国外信息安全行为的相关文献进行梳理,采用问卷调查和结构方程方法,以期解决社交网络中信息安全行为的影响因素,为相关研究提供参考。

3 研究模型及问卷设计

3.1 文献回顾

3.1.1 社交网络中感知威胁对个人信息安全保护意愿的影响　社交网络中感知威胁是指当用户感知到社交网络中存在有害内容或风险时,会采取相应的措施来应对。P. A. Rippetoe 等学者认为当用户对信息安全威胁的感知加剧时,个人将采取更加积极的行为来摆脱威胁[18];H. Liang 等学者认为感知威胁对采取保护行为起积极作用[19]。但是,东方用户和西方用户在社交网络内容方面存在着明显的差异,不同社会的用户在面对社交网络威胁时会选择不同的策略来应对[20];中国用户在快速发展的互联网社会中相对欧美国家的个人信息安全保护意识较弱,在面对社交网络上不同内容时中国用户很难分辨哪些是具备威胁性

的,这就导致用户信息安全遭到侵犯[21];H. Liang 等学者还认为感知威胁可以作为变量引入保护动机理论模型中,如果社交网络用户认为信息安全风险发生的可能性很高,但是用户不认为这会给自己带来严重的威胁,或者认为信息安全风险的影响严重,但是发生在自己身上的概率极低,那么都可能不会产生信息安全保护意愿,只有当用户切实感知到信息安全风险时,才可能产生信息安全保护意愿[13]。因此,基于上述文献的研究结果,本文认为社交网络中感知威胁正向影响社交网络用户的个人信息安全保护意愿。

3.1.2 社交网络中反应效能对个人信息安全保护意愿的影响 社交网络中反应效能是指用户面对自己采取的行为认知,换句话说如果用户认为自己采取的行为措施很有用,那么用户就会越早地采取这种行为。很多用户在使用社交网络时,从来没有使用过安全扫描软件或仅仅使用盗版软件对当前所用网站进行安全扫描,这使得他们更容易遭到信息安全的威胁[22];使用有效的技术工具可以大大降低用户使用社交网络的风险,如定期更改社交网络平台密码、使用防火墙和定期备份系统等[23];C. Yoon 等学者认为反应效能正向影响信息安全行为意愿[24];K. Witte 认为反应效能的评估是一种认知过程,在此过程中,个体对反应威胁的能力形成了思考,导致个体最终对反应效能的认知决定了他们处理威胁的方式[25]。只有相信信息安全行为的作用,认为安全行为对信息安全有利,个人才会产生采取这种行为的意愿。如果个体不相信行为是有效的,即便担心信息安全,也不一定具有保护意愿和采取信息安全的保护行为。因此,基于上述文献的研究结果,本文认为社交网络中的反应效能正向影响社交网络用户的个人信息安全保护意愿。

3.1.3 社交网络中自我效能对个人信息安全保护意愿的影响 社交网络中自我效能是指一个人在社交网络的特定情景中从事某种行为并取得预期结果的能力,它在很大程度上指个体自己对自我有关能力的感觉,也就是对自己在社交网络使用中的成功自信程度,自我效能是社会认知理论和保护动机理论的核心部分,很多学者通过研究已经证实自我效能对信息安全意愿行为具有很大的影响。J. Schaubroeck 等学者认为,由文化差异造成的东西方社会成员信息素质不对等在自我效能中扮演着重要的角色[26];M. Workman 等学者认为,自我效能高的用户使用互联网时更倾向于采取信息安全保护行为[27];A. C. Johnston 等结合保护动机理论,认为由于社交网络用户在接收隐私安全保护措施时,需要进行威胁评估,并且用户行为本身容易受到自身环境影响,自我效能将正向影响用户的信息安全意愿行为[5]。自我效能较高的个体在采取信息安全行为时,往往会信心满满。同理,如果在社交网络中个体具有较高的自我效能,那么将会更有利于采取信息安全的行为。因此,基于上述文献的研究结果,本文认为社交网络中自我效能正向影响个人信息安全保护意愿。

3.1.4 社交网络中回避行为对个人信息安全保护意愿的影响 社交网络中回避行为是指在不同程度上拒绝使用社交网络,特别是社交网络中在线支付等敏感操作,以此来防范社交网络中用户信息安全风险。回避行为的作用类似于从众效应,社交网络中个人行为无意识地受到大多数人行为影响,而不论这个行为是否正确。H. Liang 等学者将用户的回避行为描述为一个正态的正反馈循环,使用户能够全面地理解信息威胁的规避[13];Y. Chen 等学者认为避免不同程度地使用互联网是信息安全的一种应对策略,他们将回避定义为一种应对行为,通过不使用社交网络来防范信息安全威胁[6]。T. Hamamura 等学者认为与西方人相比,东方人有更强的回避意愿[28]。受传统文化影响,很多中国用户一直希望自己能够避免直接面对社交网络中的信息安全问题。社交网络平台上,网络诈骗行为屡见不鲜,中国用户因为个人财富较少,所以更容易担心威胁而避免使用社交网络。如果一个社交网络用户认为大多数人通过拒绝使用社交网络来保护自身信息安全,那么他会对信息安全保护意愿产生更强烈的抵制。因此,基于上述文献的研究结果,本文认为回避行为反向影响社交网络用户的个人信息安全保护意愿。

3.1.5 社交网络中个人信息安全保护意愿对个人信息安全保护行为的影响 信息安全保护意愿是指可以表现为采取信息安全保护行为的动机,在这项研究中,我们不区分意愿和动机。意愿是用户对是否使用社交网络的心理倾向,这种心理倾向也包含用户使用社交网络的行为倾向。F. Kujur 等学者发现在社交网络中,使用意愿、信息内容、风险性、娱乐性会影响用户使用社交网络的行为,但是用户对社交网络的使用意愿则是影响用户使用行为的最关键因素[29];I. Ajzen 认为意愿行为是一个强大的实际行为的预测,它能够在最大程度上保证行为的实现[30];E. V. Gool 等学者通过研究青少年在社交网络上分享信息行为发现,青少年分享信息的意愿是影响青少年在社交网络上主动分

享信息行为的最关键变量[31]。因此,与以往其他学者的研究相一致,我们认为具有较强信息安全保护意愿的用户更有可能采取保护个人信息安全的意愿行为。基于上述文献的研究结果,本文认为信息安全保护意愿正向影响社交网络用户的信息安全保护行为。

3.2 研究模型

根据上文提出的研究假设,本文以社会认知理论中的自我效能变量和保护动机理论中的感知威胁、反应效能变量为基础,引入新变量回避行为作为整个模型的自变量,以用户信息安全行为意愿作为中介变量,以用户信息安全行为作为因变量,构建社交网络中个人对信息安全行为影响因素的理论模型,如图 1 所示。为检验潜在变量之间的因果关系,本研究采用结构方程模型作为数据处理方式,并运用验证性因子分析对数据的信度与效度进行检验。

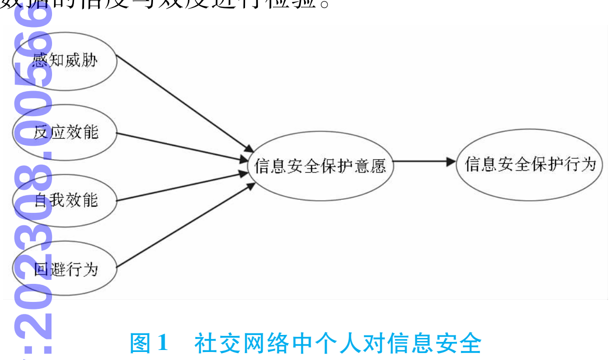


图 1　社交网络中个人对信息安全行为影响因素模型

3.3 调查问卷设计

为确保实证研究结果的可信性,本文参照 Y. Chen[6]、张晓娟[32]等学者的研究成果,设计了适合社交网络个人信息安全行为影响因素的调查问卷。问卷包括两个部分:第一部分共 6 道问项,为样本基本信息;第二部分为变量问项,共有 6 个变量,每个变量设计 5 个问题,共 30 个问题。问项采用李克特 7 级量表形式,每个项目由一组陈述句组成。在大量发放问卷前,笔者通过预调研,修正了问卷中存在的问题,如专业术语较难被受调查者理解、问项表述模糊、问项选项区分度较低等,最后才大量发放。本次调研以青年群体中使用社交网络用户的群体作为调查对象,通过各大社交媒体平台征集受访者。

4 实证研究

4.1 数据收集与研究方法

调查过程中,共发放问卷 450 份,回收后对其进行鉴别和筛选,最后得到有效问卷 385 份,有效回收率为 85.6%。本次调查的受访者女性人数比男性人数多,分别占比为 61.0 % 和 39.0%;受访者年龄为 18 – 30 岁的人数最多,所占百分比为 76.1%;受访者教育程度为本科的人数最多,所占百分比为 66.8%;受访者的职业为学生的人数最多,所占百分比为 53.2%;受访者使用社交网络的时间长度为 6 年以上的人数最多,所占百分比为 47.5%;受访者每天使用社交网络的频次为 7 次的人数最多,所占百分比为 32.7%。具体统计如表 1 所示:

表 1　调查样本描述性统计

统计量		频次	比例
性别	男	150	39%
	女	235	61%
年龄	18 岁以下	30	7.8%
	18 – 30 岁	293	76.1%
	31 – 40 岁	43	11.2%
	41 – 50 岁	13	3.4%
	50 岁以上	6	1.6%
受教育程度	大专及以下	52	13.5%
	本科	257	66.8%
	硕士	74	19.2%
	博士	2	0.5%
职业	教师或科研人员	18	4.7%
	公务员	26	6.8%
	企业职员	94	24.4%
	学生	205	53.2%
	医生	4	1%
	自由职业者	16	4.2%
	其他	22	5.7%
使用社交网络的时间长度	1 – 4 年	55	14.3%
	4 – 5 年	86	22.3%
	5 – 6 年	61	15.8%
	6 年以上	183	47.5%
每日使用社交网络的频次	0 次	2	0.5%
	1 – 2 次	91	23.6%
	3 – 4 次	93	24.2%
	5 – 6 次	73	19%
	7 次	126	32.7%

4.2 验证性因子分析

对本文所构建的测量模型进行验证性因子分析。通过 Cronbach's α 系数检验,数据具有可靠性(Cronbach's α > 0.7),可以进行下一步的数据分析。各变量之间的相关矩阵如表 2 所示,从表 2 的数据可以看出,各因素 AVE 开根号值均大于所在列和行相关系数,表明本研究的各个因素之间具有良好的区别效度。

表 2 变量相关矩阵(区别效度检验)

	感知威胁	反应效能	自我效能	回避行为	信息安全保护意愿	信息安全保护行为
感知威胁	**0.782**					
反应效能	.370 **	**0.822**				
自我效能	.387 **	.386 **	**0.836**			
回避行为	-.296 **	-.289 **	-.350 **	**0.823**		
信息安全保护意愿	.542 **	.616 **	.545 **	-.432 **	**0.850**	
信息安全保护行为	.429 **	.476 **	.474 **	-.388 **	.567 **	**0.817**

注:**表示 $p < 0.01$,加粗黑体字数值为 AVE 开根号值,其他数值为相关系数

由表 3 可知,感知威胁、反应效能、自我效能、回避行为、信息安全保护意愿、信息安全保护行为的各个题项标准化因素负荷在 0.738 - 0.889 之间,均大于 0.7,CR 分别为 0.887、0.912、0.921、0.913、0.928、0.909,均大于 0.7,AVE 分别为 0.612、0.675、0.699、0.678、0.722、0.668,均大于 0.5,表明各个因素均具有良好的收敛效度。

表 3 验证性因素分析结果

因素	项目	非标准化负荷	S. E.	C. R.	P	标准化负荷	CR	AVE
感知威胁	Q1	1				0.738	0.887	0.612
	Q2	1.152	0.073	15.757	***	0.823		
	Q3	1.129	0.072	15.793	***	0.825		
	Q4	1.041	0.07	14.963	***	0.782		
	Q5	0.963	0.068	14.097	***	0.739		
反应效能	Q6	1				0.824	0.912	0.675
	Q7	1.081	0.059	18.435	***	0.811		
	Q8	1.059	0.054	19.444	***	0.841		
	Q9	1.034	0.058	17.791	***	0.791		
	Q10	1.096	0.056	19.433	***	0.841		
自我效能	Q11	1				0.801	0.921	0.699
	Q12	1.122	0.06	18.852	***	0.844		
	Q13	1.108	0.058	19.084	***	0.852		
	Q14	1.133	0.059	19.315	***	0.859		
	Q15	1.061	0.058	18.216	***	0.823		
回避行为	Q16	1				0.789	0.913	0.678
	Q17	1.058	0.054	19.603	***	0.889		
	Q18	1.066	0.056	19.006	***	0.867		
	Q19	0.982	0.059	16.717	***	0.784		
	Q20	0.946	0.057	16.628	***	0.781		
信息安全保护意愿	Q21	1				0.858	0.928	0.722
	Q22	1.049	0.049	21.566	***	0.848		
	Q23	0.999	0.045	22.174	***	0.862		
	Q24	1.094	0.05	21.969	***	0.857		
	Q25	1.032	0.05	20.474	***	0.823		
信息安全保护行为	Q26	1				0.768	0.909	0.668
	Q27	1.078	0.063	17.112	***	0.825		
	Q28	1.154	0.068	16.853	***	0.815		
	Q29	1.204	0.066	18.341	***	0.876		
	Q30	1.092	0.066	16.45	***	0.798		

注:***表示 $p < 0.001$

4.3 模型检验

本次研究采用 AMOS 软件进行结构方程建模，并验证这些变量之间的关系。根据本研究的假设，在概念模型提出的基础上运用 AMOS23.0 建立了待验证的完整结构方程模型。将数据代入，得到图 2 所示的结构方程模型。模型的适配度指标见表 4。

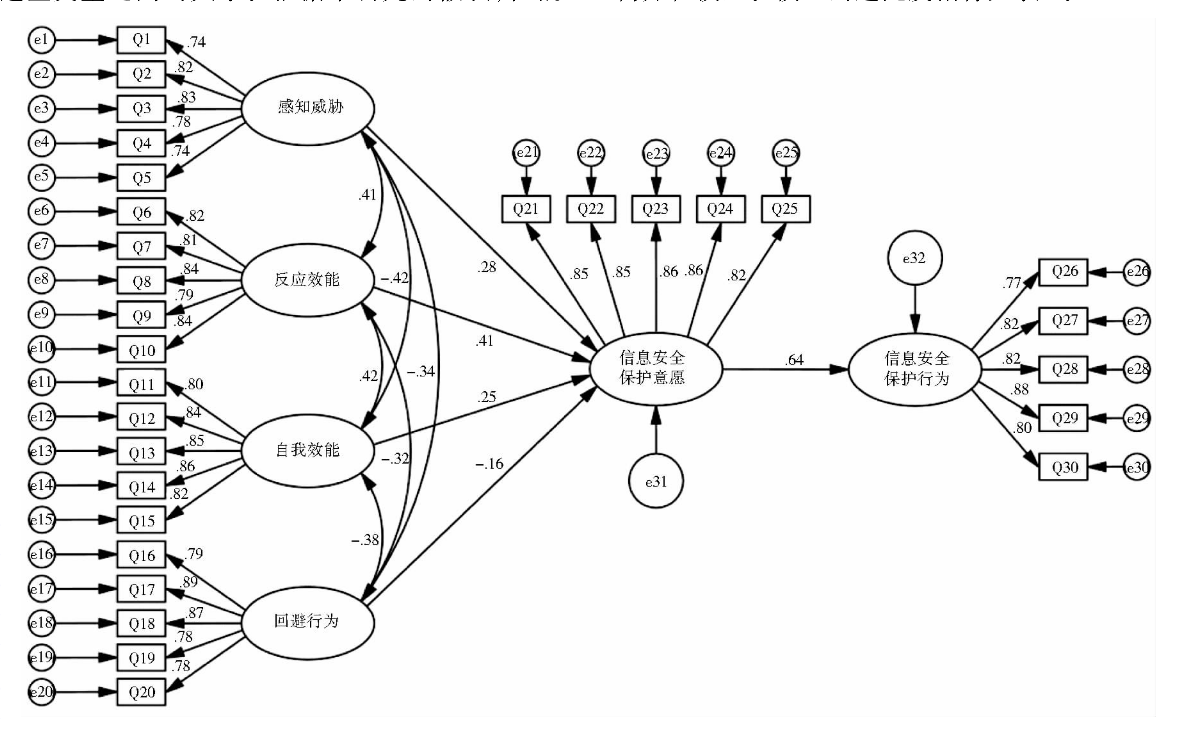


图 2 结构方程模型

从表 4 的统计量可以看出，研究理论模型的适配度指标基本达到标准，模型适配度良好。由表 5 可知，感知威胁对信息安全保护意愿（β＝0.279，p＜0.001）具有显著正向影响，假设成立；反应效能对信息安全保护意愿（β＝0.406，p＜0.001）具有显著正向影响，假设成立；自我效能对信息安全保护意愿（β＝0.250，p＜0.001）具有显著正向影响，假设成立；回避行为对信息安全保护意愿（β＝－0.158，p＜0.001）具有显著负向影响，假设成立；信息安全保护意愿对信息安全保护行为（β＝0.644，p＜0.001）具有显著正向影响，假设成立。

表 4 结构方程适配度检验

模型拟合系数	统计值	最优标准值	拟合效果
Chi-square	475.088	–	–
degrees of freedom	394	–	–
X^2/df	1.206	＜2	合格
RMSEA	0.023	＜0.05	合格
GFI	0.928	＞0.9	合格
CFI	0.990	＞0.9	合格
IFI	0.990	＞0.9	合格
TLI	0.989	＞0.9	合格
NFI	0.945	＞0.9	合格

表 5 模型验证

路径			标准化系数	非标准化系数	S. E.	C. R.	P	假设
信息安全保护意愿	←	感知威胁	0.279	0.290	0.047	6.105	***	成立
信息安全保护意愿	←	反应效能	0.406	0.392	0.044	8.883	***	成立
信息安全保护意愿	←	自我效能	0.250	0.242	0.043	5.606	***	成立
信息安全保护意愿	←	回避行为	－0.158	－0.133	0.034	－3.868	***	成立
信息安全保护行为	←	信息安全保护意愿	0.644	0.597	0.051	11.615	***	成立

注：***表示 p＜0.001

5 讨论分析

从上述各图表的数据结果可以看出，本文提出的假设的检验结果均得到数据支持。数据分析结果表明，信息安全保护意愿正向影响信息安全保护行为（β＝0.64）。外部潜在变量对社交网络用户信息安全保

护意愿的正向影响作用系数依次为反应效能（β = 0.41）、感知威胁（β = 0.28）、自我效能（β = 0.25）；其中，社交网络用户的回避行为对信息安全保护意愿产生负向影响（β = −0.16）。

5.1 反应效能对社交网络用户信息安全保护意愿的影响

社交网络中用户反应效能对信息安全保护意愿产生正向影响，影响系数为0.41，显著性P值<0.001，达到了显著性要求。这一数据结果表明，用户的反应效能通过对信息安全保护意愿的影响，间接地影响用户的信息安全保护行为。这一结论与K. Witte对信息安全意愿的研究具有某种程度的一致性，他认为由于用户在反应效能评估的过程中对反应威胁的能力形成了思考，导致用户最终对反应效能的认知决定了他们处理威胁的方式[25]。

这一数据分析结果说明，如果用户认识到使用一些安全扫描软件或其他社交网络安全保护工具，或了解社交网络的安全政策，可以帮助用户检测或降低社交网络使用中的安全风险，那么用户就更愿意使用社交网络。因此，社交网络平台应该增强与安全扫描模块的合作，对用户的个人信息安全进行保护和进行安全风险提示，完善社交网络的安全保护政策，并规范社交网络平台安全管理体系和建立用户个人信息安全的保障机制，从而降低社交网络使用中的安全风险。此外，政府及行业监管平台也应该向社交网络使用者宣传个人信息安全的重要性，并通过培训提高用户对信息安全保护及隐私保护的相关手段、工具及操作指导，这样不但可以形成积极的信息安全保护行为意愿，还可以更好地促动信息安全和隐私保护相关制度的建设。

5.2 感知威胁对社交网络用户信息安全保护意愿的影响

社交网络中用户感知威胁对信息安全保护意愿产生正向影响，影响系数为0.28，显著性P值<0.001，达到了显著性要求。这一数据结果表明，用户的感知威胁能帮助用户在社交网络中自动抵制不认识的人所发出的加入好友请求，避免个人信息被不怀好意的人盗用和篡改，在一定程度上对用户信息安全保护起到了较为重要的作用。这一结果与张晓娟的研究具有一定的相似性，她将感知威胁作为影响用户信息安全意愿的正向因素，并认为信息安全意愿越强，越有动机采取信息安全行为[7]。

这一数据分析结果说明，在用户使用社交网络过程中，感知威胁会正向影响其所推荐的信息安全风险规避方案。引入威胁评估过程可以使用户对安全保护行为效能的认知产生认同感，进一步对其安全保护行为的采纳意愿产生积极作用。目前年轻人和老年人群体是目前社交网络中的弱势用户群体，其感知威胁的能力相对较弱，容易轻信陌生人。年轻人经常通过社交网络与网友见面，个人人身安全受到威胁；老年人通过社交网络容易泄露个人账户和隐私信息，个人财务安全受到威胁。国家及行业层面加强社交网络中弱势群体的感知威胁能力变得尤为重要，政府和企业应该重点加强对弱势群体的信息安全保护的培训及宣传引导，使弱势群体在使用中意识到社交网络中存在的潜在风险，并采取适当的自我保护机制及树立风险防范意识。

5.3 自我效能对社交网络用户信息安全保护意愿的影响

社交网络中用户自我效能对信息安全保护意愿产生正向影响，影响系数为0.25，显著性P值<0.001，达到了显著性要求。该数据分析结果表明自我效能在用户信息安全保护意愿中产生了关键作用。这一结论与M. Workman等学者的研究结论相一致，他们认为自我效能高的用户在使用互联网时，更倾向于采取信息安全行为[27]。

这一数据分析结果说明，社交网络中用户的自我效能主要体现在用户能够灵活掌握社交网络中的各项操作技能，并能识别和应对社交网络中所遇到的各种安全威胁，了解社交网络的安全准则等。因此对于社交网络平台运营商来说，要想保证平台的日常活跃量，就要充分考虑社交网络平台的易用性、功能性和实用性，使用户通过简单的操作，就可以对个人信息安全进行保护；同时网络社交平台的运营商也应做好相应的引导工作，帮助降低用户各种可能出现的信息安全及个人隐私的泄露风险，并通过社交网络平台简化易用的自我风险保护操作功能及风险提示功能，从平台的设计及信息安全保护技术等方面防止各种可能出现的安全隐患，帮助用户规避在平台使用中可能出现的各种风险及隐患，从而让更多的用户使用社交网络。

5.4 回避行为对社交网络用户信息安全保护意愿的影响

社交网络中用户回避行为对信息安全保护意愿产生反向影响，影响系数为−0.16，显著性P值<0.001，达到了显著性要求。这一数据分析结果表明回避行为对用户信息安全意愿产生了消极影响。这一假设也支

持前人的研究观点，如学者 H. Liang 等在相关研究中指出，人们的回避动机与他们所采纳的行为有着密切的关系[13]；除此之外 Y. Chen 等学者通过研究得出受传统文化影响，回避在中国是一种非常普遍的行为[6]，因此可以看出回避行为会对社交网络中用户的信息安全行为产生直接影响。

社交网络平台不同于传统的社交手段，它具有即时性、广泛性、传播性和风险性等众多特点。随着信息化的快速发展，各地区用户与社交网络的接触也随之变多，由于大部分用户缺乏对网络信息真伪的识别能力，导致社交网络上的诈骗和隐私泄露等问题频频发生，以至于很多用户采取拒绝使用社交网络回避行为来保护自身的隐私和财务安全。在信息化时代，这部分用户有着被边缘化的风险。面对社交网络中存在的潜在信息安全威胁，广大用户可以通过增强自身信息安全自我保护素养和风险识别素养，以及使用一些安全扫描工具进行有效反击；社交网络工具应加强发展网络信息安全保护技术。

5.5 信息安全保护意愿对社交网络用户信息安全保护行为的影响

社交网络中用户信息安全保护意愿对信息安全保护行为产生正向影响，影响系数为 0.64，显著性 P 值 <0.001，达到了显著性要求。在社交网络环境中，用户信息安全行为主要是由其意愿所决定，社交网络用户的感知威胁、反应效能、自我效能以及回避行为通过用户的信息安全保护意愿间接影响社交网络用户的信息安全保护行为。其中，意愿起到了很好的中介变量作用。此结论与国外学者 H. Liang 等人在信息安全行为领域中的研究相一致，即用户在使用社交网络中信息安全意愿越强，就越容易采纳信息安全行为[13]。

这一数据分析结果说明，社交网络平台有必要向广大用户传达信息安全的现状以及信息安全的重要性，使用户意识到恰当的行为有助于保护个人信息安全。此外，用户应该积极学习有关信息安全其他方面的知识，主动接受个人信息安全培训，在使用社交网络时，用户要仔细阅读相关隐私协议，知悉隐私设置方法，形成个人信息保护意识。同时，社会也应加强信息安全立法，比如 2017 年 6 月 1 日起开始实施《网络安全法》就是法律人士赞同的增强信息安全保护的重要举措。

6 研究结论

本文的理论贡献在于，以社会认知理论和保护动机理论为基础构建社交网络个人信息安全行为影响因素模型，分析了社交网络用户信息安全行为的影响因素。数据分析结果表明，社交网络中的感知威胁、反应效能和自我效能对用户信息安全保护意愿产生直接正向影响；回避行为对信息安全意愿产生消极影响，对信息安全保护行为产生间接影响；信息安全保护意愿是社交网络个人信息安全行为影响因素模型的中介变量。本研究为社交网络中用户信息安全行为研究提供了新的行为分析模型。

本文的实践价值在于，运用了结构方程和问卷调查方法，探讨社交网络个人信息安全行为影响因素。实证分析表明：用户应认识和使用个人信息安全保护工具以降低社交网络使用中的安全风险；引入威胁评估过程可以使用户对安全保护行为效能的认知产生认同感；网络社交平台的运营商也应做好相应的引导工作，帮助降低用户各种可能出现的信息安全及个人隐私的泄露风险；面对社交网络中存在的潜在信息安全威胁，广大用户可以通过增强自身信息安全自我保护素养和风险识别素养。

本文在研究中也存在一定的局限性。在研究中，实证研究样本主要来自高校学生，他们每天使用社交网络的时间普遍较长，而其他年龄、其他职业的样本相对较少，这可能会导致本研究的影响因素针对不同群体的普适性。在后续的研究中，笔者将会扩大问卷调查对象的群体范围，以更好地验证模型对不同群体的适用性。同时，影响因素模型在未来研究中将适当增加变量，以增加模型分析的粒度。

参考文献：

[1] 腾讯科技. 2017 年度互联网安全报告[EB/OL]. [2018－01－19]. http://tech.qq.com/a/20180119/012161.htm.
[2] 中国互联网络信息中心. 第 41 次中国互联网络发展状况统计报告[EB/OL]. [2017－01－22]. http://www.cac.gov.cn/2018-01/31/c_1122347026.htm.
[3] 孟晓明，贺伟. 社交网络大数据商业化开发利用中的个人隐私保护[J]. 图书馆论坛，2015(6):67－75.
[4] BANDURA A. Human agency in social cognitive theory[J]. American psychologist, 1989, 44(9):1175－1184.
[5] JOHNSTON A C, WARKENTIN M. Fear appeals and information security behaviors: an empirical study[J]. MIS quarterly, 2010, 34(3):549－566.
[6] CHEN Y, ZAHEDI F M. Individuals' Internet security perceptions and behaviors: polycontextual contrasts between the United States and China[J]. MIS quarterly, 2016, 40(1):205－222.
[7] 张晓娟. 隐私关注对智能手机用户信息安全行为意向的影响研究[J]. 情报理论与实践，2017(11):3－10.

[8] 王璐瑶. 恐惧诉求对社交网络用户隐私安全保护行为的影响研究[J]. 情报杂志,2016(12):2-6.

[9] 罗力. 社交网络中用户个人信息安全保护研究[J]. 图书馆学研究,2012(14):36-40.

[10] BOYD D M,ELLISON N B. Social network sites:definition,history,and scholarship[J]. Journal of computer-mediated communication,2007,13(1):210-230.

[11] 刘志辉,张志强. 作者关键词耦合分析方法及实证研究[J]. 情报杂志,2014(12):268-275.

[12] HOLT B E, BROWN H C. Animal drive and the learning process, an essay toward radical empiricism[J]. Journal of nervous and mental disease,1933,78(5):586-600.

[13] LIANG H, XUE Y. Avoidance of information technology threats: a theoretical perspective[J]. MIS quarterly,2009,33(1):71-90.

[14] INKELES A. Becoming modern: individual change in six developing countries[J]. Ethos,2010,3(2):323-342.

[15] Abbassi A. Culture and anxiety:a cross-cultural study[J]. Journal of professional counseling practice theory & research,2007,35(1):26.

[16] WONG P T P,WONG L C J, SCOTT C. Beyond stress and coping: the positive psychology of transformation[A]//Handbook of multicultural perspectives on stress and coping. New York:Routladge,2006:1-26.

[17] ROGERS R W,CACIOPPO J T,PETTY R. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation[A]//Social psychophysiology. New York:Guilford Press,1983.

[18] RIPPETOE P A,ROGERS R W. Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat[J]. Journal of personality and social psychology,1987,52(3):596-604.

[19] LIANG H,XUE Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective[J]. Journal of the Association for Information Systems,2010,11(7):394-413.

[20] HEPPNER P P, HEPPNER M J, LEE D G, et al. Development and validation of a collectivistic coping styles inventory[J]. Journal of counseling psychology,2006,53(1):107-125.

[21] Economist intelligence unit. Digital economy rankings 2010 beyond e-readiness[EB/OL]. [2018-01-19]. http://www-935.ibm.com/services/us/gbs/bus/pdf/eiu_digital-economy-rankings-2010_final_web.pdf.

[22] BSA. Sixth annual bsa and idc global software piracy study[EB/OL]. [2018-01-19]. http://www.global.bsa.org/globalpiracy2008/index.html.

[23] IFINEDO P. Information systems security policy compliance: an empirical study of the effects of socialisation,influence,and cognition[J]. Information & management,2014,51(1): 69-79.

[24] YOON C,HWANG J W,KIM R. Exploring factors that influence students' behaviors in information security[J]. Journal of information systems education,2012,23(4):407-415.

[25] WITTE K. Putting the fear back into fear appeals: the extended parallel process model[J]. Communication monographs,1992,59(4):329-349.

[26] SCHAUBROECK J, LAM S S, XIE J L. Collective efficacy versus self-efficacy in coping responses to stressors and control: a cross-cultural study[J]. Journal of applied psychology,2000,85(4):512-525.

[27] WORKMAN M,BOMMER H H,STRAUB D. Security lapses and the omission of information security measures: a threat control model and empirical test[J]. Computers in human behavior, 2008,24(6):2799-2816.

[28] HAMAMURA T, MEIJER Z, HEINE S J,et al. Approach-avoidance motivation and information processing: a cross-cultural analysis[J]. Personality and social psychology bulletin,2009,35(4):454-462.

[29] KUJUR F,SINGH S. Engaging customers through online participation in social networking sites[J]. Asia pacific management review,2017,22(1):16-24.

[30] AJZEN I. The theory of planned behavior[J]. Organizational behavior & decision processes,1991,50:179-211.

[31] GOOL E V,OUYTSEL J V,PONNET K,et al. To share or not to share? adolescents' self-disclosure about peer relationships on Facebook: an application of the prototype willingness model[J]. Computers in human behavior,2015,44(3):230-239.

[32] 张晓娟. 基于社会认知理论的智能手机用户信息安全行为意愿研究[J]. 现代情报,2017(9):2-5.

作者贡献说明:

王晰巍: 提出研究命题、研究思路,撰写论文及修订论文最后版本;

王雷: 负责论文撰写、修改及数据采集;

贾若男: 协助进行论文的收集和整理;

王铎: 论文英文内容的翻译及处理。

An Empirical Study on the Influencing Factors of the Security Behavior in Personal Information in Social Networks

Wang Xiwei[1,2] Wang Lei[1] Jia Ruonan[1] Wang Duo[1]

[1] School of Management, Jilin University, Changchun 130022

[2] Big Data Management Research Center, Jilin University, Changchun 130022

王晰巍，王雷，贾若男，等.社交网络中个人信息安全行为影响因素的实证研究[J].图书情报工作,2018,62(18):24－33.

Abstract: [**Purpose/significance**] With the gradual increasing number of social network users, the research on the behavior of personal information security in social network has a positive role in better helping social network users to avoid social network security risks and urging the social network platform developers to improve information security technology. [**Method/process**] Based on the theory of social cognition and protective motivation, this paper constructs a model of influencing factors of social network personal information security behavior, and tests the applicability of the model by the survey of questionnaire and structural equation method. [**Result/conclusion**] The results show that response efficiency is the most important factor which influences the behavior of personal information security protection in social networks, and the perceived threat and self-efficacy have a positive effect on personal information security protection willingness. But avoidance behavior has a negative impact on the willingness to protect information security, and the users' willingness to protect information security has a positive impact on the behavior of information security protection.

Keywords: social network　personal information security　behavior　influencing factor

图书馆事业发展南京宣言(2018)

当前,中国特色社会主义已进入新时代,中国图书馆事业也正在进入一个新时代。新时代的图书馆事业要有新的使命、新的目标和新的担当。科研教育与文化事业的蓬勃发展,信息通讯技术的广泛普及与应用,用户对文献信息资源与服务的新需求,都对图书馆事业的发展提出了新的挑战与新的发展动力。图书馆事业发展也正在孕育新的生机和活力。

为重新认识新时代图书馆事业的战略定位,加快从传统图书馆到新时代图书馆的转型变革,更大地发挥图书馆新的作用,来自于全国各类型图书馆和图书馆学教学、研究机构的图书馆实务、理论与教育工作者160余人,于2018年6月20日,在南京大学召开了"新时代新发展:服务 效能 法制"中国图书馆事业发展高层论坛。经过研讨,与会专家和代表形成如下共识与建议:

1. 新时代图书馆事业责任重大使命光荣。新时代的图书馆事业,机遇与挑战并存。图书馆界同仁须认清发展方向,明确自身的定位与时俱进,重塑形象,勇于担当,加强社会责任感,更有效地发挥自身的功能,不断创新发展,不断提升自身的服务效能,增强自身的社会价值和社会贡献度,将危机转变成契机。

2. 进一步加强图书馆的法制建设。图书馆法规是图书馆事业可持续健康发展的重要保障。《中华人民共和国公共图书馆法》的颁布具有里程碑意义,各级政府和各级图书馆应依法履行职责,推进中国图书馆事业发展。同时应从实践和理论两个方面继续推动良好的图书馆法律环境建设,促进包括各类型图书馆在内的"图书馆法"的出台,构建完备的图书馆法律体系,将图书馆事业的发展纳入法治化、规范化、有序化的轨道,保障图书馆事业的可持续健康发展。

3. 加快新技术的研发与应用。以互联网、大数据、人工智能为代表的新技术有助于图书馆核心价值和功能的加快实现。新技术的发展及在图书馆的广泛应用,已经并将不断推动图书馆事业发展的进程,推动图书馆业务能力与服务能力的提升。新技术是图书馆实现自身愿景与目标的助推器和加速器。图书馆员应积极拥抱新技术,积极吸纳和应用新技术,加快新技术应用的进程,掌控新技术,为我所用。

4. 进一步强化服务能力建设。为用户提供基于不同需求、不同层次、不同方式的图书馆服务是图书馆的核心价值和根本任务。图书馆事业的发展必须坚持以人为本,坚持以用户为中心,恪守普遍、开放、共享、平等的图书馆服务原则,不断深化服务内容,扩展服务方式,提升服务能力,保障服务效果。

5. 图书馆必须走高质量发展道路。应鼓励图书馆各种类型的创新,注重创新成效,不断提升图书馆服务效能,增加图书馆自身价值。人才是图书馆高质量发展的基础,图书馆必须重视各种类型人才建设、加强人才梯队和团队建设。图书馆员应爱岗敬业,勤奋奉献,加强专业研究和专业能力的提升,努力使自己成为专家型馆员。

6. 进一步推动图书馆的共建共享建设。公共图书馆、高校图书馆、专业图书馆应该得到均衡、充分的发展。应加强图书馆事业的顶层设计,夯实图书馆基础工作,依法做好统计和评估工作,加强图书馆之间的交流与协作,协同开展图书馆的各项业务与服务工作。

7. 进一步发挥多元力量办好图书馆。社会力量是图书馆事业发展的重要参与者。随着中国经济、文化的发展,社会上越来越多的有识之士愿意为图书馆事业贡献一份力量。图书馆界应主动加强与社会力量的跨界合作,充分发挥社会力量创办图书馆的积极性和所发挥的不可替代的作用。

8. 进一步加强图书馆学教育和研究。图书馆学教育要不辱使命,大胆改革课程体系,完善知识结构,鼓励在学科核心内容基础上加以拓展。图书馆研究者应大力倡导图书馆学及交叉学科的研究,加强学科术语名词规范和基本理论研究,加强教学、科研和新技术的应用研究。应坚持理论与实际密切结合和互动,理论研究、应用研究、技术开发并重,研究解决图书馆事业当前和未来发展面临的主要困境和存在的问题,以研究促发展,推出更多的前瞻性研究成果。